WE CLAIM

1. A public key certificate generation method by a registration authority and an issuing authority in the public key infrastructure, comprising the steps of:

sending a certificate issuing request including a registration contents of a public key certificate and an information content guaranteed by the registration authority, to the issuing authority in a registration authority; and

generating a public key certificate including the registration contents described in the certificate issuing request, the information guaranteed by the registration authority, issuing contents issued by the issuing authority, and a signature to the issuing contents in the issuing authority.

2. The public key certificate generation method as claimed in Claim 1, wherein

an identifier is predetermined so as to specify information to be described in the public key certificate; and

the registration authority includes the signature to the information guaranteed by the registration authority and the identifier as the information guaranteed by the registration authority.

3. The public key certificate generation method as claimed in Claim 1, wherein

the registration authority applies a hash function to the information guaranteed by the

registration authority so as to obtain a hash value and generates a signature for this hash value, so that the hash value and the signature are included in the information guaranteed by the registration authority.

4. A public key certificate validation method for verifying a public key certificate generated according to the public key certificate generation method claimed in Claim 1, wherein

a verifying person verifies the signature of the issuing authority and the signature of the registration authority attached to the entire public key certificate; and

confirms the registration contents signed by the registration authority and the issuing contents signed by the issuing authority.

5. A public key certificate validation method for verifying a public key certificate generated according to the public key certificate generation method claimed in Claim 2, wherein a verifying person performs the steps of:

using the identifier to fetch from the public key certificate, information signed by the registration authority;

obtaining a hash value of the fetched information;

decoding the registration authority signature contained in the information guaranteed by the registration authority, by using a public key of the

registration authority; and

checking whether the hash value is identical to the decoded value, thereby verifying the information to be guaranteed by the registration authority.

6. A public key certificate validation method for verifying a public key certificate generated according to the public key certificate generation method claimed in Claim 3, the method comprising the steps of:

obtaining a hash value of information described in the public key certificate; and

comparing the hash value contained in the information guaranteed by the registration authority to the hash value obtained;

thereby performing identification of the information to be guaranteed by the registration authority and verifying the identified information.

7. The public key certificate validation method as claimed in Claim 4, the method further comprising the steps of:

constructing and verifying a path from the certificate authority trusted by a verifying person, up to the public key certificate;

verifying the registration authority signature described in the public key certificate using the public key of the registration authority; and

constructing and verifying a path from the certificate authority trusted by the verifying person

up to the public key certificate.

8. The public key certificate validation method as claimed in Claim 7, wherein the path from the certificate authority up to the public key certificate of the registration authority is performed by that according to the registration authority name described on the public key certificate, the verifying person fetches the public key certificate of the registration authority from a public key certificate database of the issuing authority.

9. The public key certificate validation method as claimed in Claim 7, wherein the path from the certificate authority up to the public key certificate of the registration authority is performed by fetching the public key certificate of the registration authority described in an extended region of the public key certificate to be verified.

10. A public key certificate invalidation method for invalidating a public key certificate generated according to the public key certificate generation method disclosed in Claim 1, wherein

a registration authority sends a certificate invalidation request to an issuing authority of its public key certificate; and

the issuing authority receives the certificate invalidation request and invalidates the public key certificate of the registration authority,

thereby invalidating the public key

certificate which has been registered by the registration authority.